UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/043,654	01/10/2002	Nelson Waldo Bunker V.	CRIT-27,301	7438

25883 7590 01/23/2006

HOWISON & ARNOTT, L.L.P
P.O. BOX 741715
DALLAS, TX 75374-1715

EXAMINER
TRAN, TONGOC

ART UNIT	PAPER NUMBER
2134	

DATE MAILED: 01/23/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 10/043,654	**Applicant(s)** BUNKER V. ET AL.	
	Examiner Tongoc Tran	**Art Unit** 2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *13 October 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-36,58,62-64,68-70,74-90 and 103-111* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-36,58,62,64,68,70,74,76-90 and 103-111* is/are rejected.

7)☒ Claim(s) *63,69 and 75* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)	4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)	5) ☐ Notice of Informal Patent Application (PTO-152)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.	6) ☐ Other: _____.

DETAILED ACTION

1. This office action is in response to Applicant's amendment filed on 10/13/2005. Claims 1-3, 5-8, 10-11, 13, 17, 18, 25, 29, 30, 58, 64,69, 70, 74, 75 and 85 have been amended. Claims 37-57, 59-61, 65-67, 71-73, 91-102 have been canceled. Claims 103-111 have been added. Claims 1-36, 58, 62-64, 68-70, 74-90 and 103-111 are pending.

Response to Arguments

2. Applicant's arguments with respect to amended claims have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 1-36 are rejected under 35 U.S.C. 102(b) as being anticipated by Gleichauf et al. (U.S. Patent No. 6,324,656).

Regarding claim 1, Gleichauf teaches a network security testing apparatus comprising:

a first tester that is adapted to communicably couple to a system under test Gleichauf, a first NVA engine coupled to network; col. 3, lines 41-67); said first tester is adapted to sequentially perform a plurality of tests on the system under test; wherein the plurality of tests adapted to return system environment information regarding the system under test; wherein each of the plurality of tests are more specific to the system under test based on information gained from a previous test (each test gathers information about network devices, services, or vulnerabilities and returns it to port database 22; col. 6, lines 22-23; col. 8, lines 12-25, each test contains different phases, active analysis phase is for the purpose of confirming the potential vulnerabilities identified by the previous output).

Regarding claim 2, Gleichauf teaches all the limitations of claim 1, Gleichauf further teaches wherein the plurity of test comprises at least three tests (col. 4, lines 9-19).

Regarding claim 3, Gleichauf teaches all the limitations of claim 1, and further teaches that the second test is based at least partially upon system environment information detected by the previous test (col. 8, lines 12-17, col. 8, lines 13-25).

Regarding claim 4, Gleichauf teaches all the limitations of claim 3, and further teaches that the system environment information includes information regarding network connectivity from the first tester to the system under test (information from first test is stored in port database 22 and identifies, for example, what ports are active on workstations connected to the network; col. 4, lines 20-30 and 40-42).

Regarding claim 5, Gleichauf teaches all the limitations of claim 3 wherein the system environment information includes network security vulnerability information (col. 8, lines 12-25).

Regarding claim 6, Gleichauf teaches all the limitations of claim 5, wherein network security vulnerability information includes connection information relating to an IP address used in the previous first test (col. 8, lines 12-25).

Regarding claim 7, Gleichauf teaches all the limitations of claim 3, and further teaches that an apparatus comprising:

a second tester that is adapted to communicably couple to a system under test (a second NVA engine coupled to network; col. 3, lines 41-67);

wherein the previous test (preliminary analysis) is executed by said first tester (first NVA engine);

wherein determination of whether the second test (either an active exploits analysis test or a repeat preliminary analysis test) is executed by said first tester or by said second tester is made based at least partially upon the system environment information (iterative process determines whether subsequent test is conducted as an active exploits test by second NVA engine or as a further preliminary analysis test by first NVA engine; col. 7, lines 55-61).

Regarding claim 8, Gleichauf teaches all the limitations of claim 3, and further teaches that the subsequent test includes execution of a test tool selected from a plurality of test tools based at least partially upon the system environment information (Gleichauf: a plurality of tests is noted by the provision of at least two examples, and it is inherent that the selection of a test tool among a plurality of test tools stems from the selection of a test from a plurality of tests, wherein the tests differ from one another as to require different tools; col. 6, lines 15-18).

Regarding claim 9, Gleichauf teaches all the limitations of claim 3, and further teaches that said first tester is adapted to execute an additional test of the plurality of tests if said first tester has not yet definitely gathered all possible system environment information about the system under test, in light of the plurality of tests (iterative process determines whether an additional test is conducted as further preliminary analysis by first NVA engine based upon whether first NVA engine has gathered all possible system environment information; col. 7, lines 55-61).

Regarding claim 10, Gleichauf teaches all the limitations of claim 2, and further teaches wherein the plurality of tests continue until all relevant information about the system under test has been collected (col. 8, lines 12-17).

Regarding claim 11, Gleichauf teaches all the limitations of claim 7, and further teaches that the subsequent test includes execution of a test tool selected from a plurality of test tools based at least partially upon the system environment information (a plurality of tests is noted by the provision of at least two examples, and it is inherent that the selection of a test tool among a plurality of test tools stems from the selection of a test from a plurality of tests, wherein the tests differ from one another as to require different tools; col. 6, lines 15-18).

Regarding claim 12, Gleichauf teaches all the limitations of claim 7, and further teaches that said first tester is adapted to execute an additional test of the plurality of tests if said first tester has not yet definitely gathered all possible system environment information about the system under test, in light of the plurality of tests (iterative process determines whether an additional test is conducted as further preliminary analysis by first NVA engine based upon whether first NVA engine has gathered all possible system environment information; col. 7, lines 55-61).

Regarding claims 13-24 and 25-36, these are a method and computer program-product versions, respectively, of the claimed apparatus above (claims 1-12). Therefore, for reasons applied above, such a claims also is anticipated.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 76-87 and 106-111 are rejected under 35 U.S.C. 103(a) as being unpatentable over Gleichauf et al (U.S. Patent No. 6,324,656) in view of Polk "Automated Tools for Testing Computer Systems Vulnerability", http://nsi.org/Library/Compsec/CSECTOOL.TEXT, December 1992.

Regarding claim 76, Gleichauf teaches a network security testing apparatus comprising a first tester that is adapted to communicably couple to a system under test, wherein said first tester is adapted to perform a test on the system under test (a first NVA engine coupled to network; col. 3, lines 41-67; col. 6, lines 8-21), wherein said first tester is adapted to make a first attempt to communicably couple to the system under test before the test (Gleichauf, col. 4, lines 56-67, NVA engine is placed outside of internal network and external to router and firewall...this placement give NVA engine a better view of devices on external network). Gleichauf does not explicitly discloses wherein said first tester is adapted to make a second attempt to communicably couple to the system under test after the test; and wherein the combination of success of the first attempt and failure of the second attempt are interpreted as detection of the test by the system under test. However, Polk discloses tests for system vulnerability may mimic an attacker or simply browse through the system in a more typical auditing fashion...(page 8, last paragraph) and "tests may be classified as passive or active...active tests are intrusive in nature; they identify vulnerability by exploiting them...active tests are more dangerous than passive tests, active tests can frequently be transformed into a Trojan horse (or network worm) with only minor modifications (page 9, 3.1, Active and Passive Testing; active testing target system-specific vulnerabilities...all active tests will be custom software (page 16, 1st paragraph). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the teaching of Gleichauf's tester placed outside of the internal for better view of the system with Polk's teaching of custom protective testing measure to ensure the system may not transformed into a network worm after the active testing is completed.

Regarding claim 77, this claim is rejected on the same basis as claim 76, Therefore, for reasons applied above, such claims also would have been obvious.

Regarding claim 78, Gleichauf teaches the limitations of claim 77, but do not explain an apparatus wherein the first attempt is made using a first originating IP address; wherein the second attempt is made using a second originating IP address that is essentially the same as the first originating IP address; wherein a third attempt to communicably couple to the system under test is made using a wherein the combination of success of the first attempt, failure of the second attempt, and success of the third attempt is interpreted as a possibility including the detection; and wherein the combination of success of the first attempt, failure of the second attempt, and failure of the third attempt is interpreted as a possibility including: a network connectivity problem between the first tester and the system under test; and the detection.

However, Polk discloses tests for system vulnerability may mimic an attacker or simply browse through the system in a more typical auditing fashion...(page 8, last paragraph, this encompass attempt is made using first IP address) and "tests may be classified as passive or active...active tests are intrusive in nature; they identify vulnerability by exploiting them...active tests are more dangerous than passive tests, active tests can frequently be transformed into a Trojan horse (or network worm) with only minor modifications (page 9, 3.1, Active and Passive Testing; active testing target system-specific vulnerabilities...all active tests will be customer software (page 16, 1st paragraph; preventive measurement encompass post testing protective measurement accessing network system using originating IP address). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the teaching of Gleichauf's tester placed outside of the internal for better view of the system with Polk's teaching of customer protective testing measure to ensure the system may not transformed into a network worm after the active testing is complete.

Regarding claim 79, this claim is rejected on the same basis as claim 78, Therefore, for reasons applied above, such claims also would have been obvious.

Regarding claims 80-87, these are a method and computer-program-product versions of the claimed apparatus above (claims 76-78). Therefore, for reasons applied above, such claims also would have been obvious.

Regarding claims 106-111, these are a method and computer-program-product versions of the claimed apparatus above (claims 76-77). Therefore, for reasons applied above, such claims also would have been obvious.

9. Claims 88-90 are rejected under 35 U.S.C. 103(a) as being unpatentable over Gleichauf (U.S. Patent No. 6,324,656) view of Srinivasan ("Binding Protocols for ONC RPC Version 2", Network Working Group RFC 1833, August 1995).

Regarding claim 88, Gleichauf discloses a network security testing apparatus comprising:

a tester (Gleichauf, network security system);

a test tool (Gleichauf, port scans);

wherein said tester is adapted to be communicably coupled to a system under test (Gleichauf, col. 2, lines 28-42); and

wherein said tester is adapted to test the system under test by execution of said test tool (Gleichauf, col. 2, lines 28-42).

But Gleichauf does not explain an application programming interface (API), adapted to interface between tester and said test tool, said API further including an API stub enabling said test tool to be executed by said tester even if the outputs of said tester do not directly corresponsed to the inputs of said test tool, and such that said test tool may be executed by said tester even if the inputs of said tester do not directly correspond to the outputs of said test tool, said API further including a common API for interfacing between the test tool and instruction provided to the test tool and wherein said tester is adapted to test the system under test by execution of said test tool.

However, Gleichauf teaches that the test tools (NVA engines) runs on a Sun based workstation and is operable remotely from the tester (col. 3, lines 30-55). As it is widely known in the art that remote programs are called using an API known as a Remote Procedure Call (RPC), the Examiner takes official notice that one of ordinary skill in the art would recognize that remote operation of a software program is accomplished on Sun based workstations using the Remote Procedure Call (RPC) API adopted by Sun Microsystems, namely ONC Binding Protocols for RPC version 3. And Srinivasan teaches the ONC Binding Protocols for RPC version 3 wherein calling a remote program requires providing a RPC program number and version for the purpose of providing the RPC services with the information it needs to identify the remote program using its lookup service. It follows that where the tester uses a RPC API to call a remote test program, the outputs from the tester will include a RPC program number and a RPC program version, whereas the tester calling a local test program would not include this information in its outputs.

Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made to provide for an application programming interface (API), wherein said API is adapted to interface between said tester and said test tool, such that said test tool may be executed by said tester even if the outputs of said tester do not directly correspond to the inputs of said test tool, and such that said test tool may be executed by said tester even if the inputs of said tester do not directly correspond to the outputs of said test tool. One would be motivated to do so for the purpose of remotely operating the test tool.

Regarding claims 89 and 90, these are a method and computer-program product versions of the claimed apparatus above (claim 88). Therefore, for reasons applied above, such claims also would have been obvious.

Claims 103-105 are rejected under 35 U.S.C. 103(a) as being unpatentable over Gleichauf et al. (U.S. Patent No. 6,324,656, hereinafter Gleichauf '656) in view of Gleichauf et al. (U.S. Patent No. 6,301,668, hereinafter Gleichauf '668).

Regarding to claim 103, Gleichauf '656 teaches an apparatus comprising:
a plurality of testers (Gleichauf '656 plurality of NVA engines; col. 3, lines 57-67); a customer profile (Gleichauf, '656, col. 3, lines 34-58)

wherein each of said plurality of testers is adapted to communicably couple to a system under test (Gleichauf '656, NVA engines each couple to the network being tested; col. 3, lines 43-50 and 57-63).

a test system under test is performed by a selected tester of said plurality of testers (Gleichauf '656, iterative process determines whether second test is conducted as an active exploits test 98 by second NVA engine or as a further preliminary analysis test 94 by first NVA engine, wherein determination is based on information in port database 22/network map; Fig. 3A; col. 5, lines 36-40; col. 6, lines 8-12 and 34-37; col. 7, lines 55-61).

Gleichauf does not explicitly teach but Gleichauf '668 teaches wherein each tester has at least one quality of communicable couple to the system under test the at least one quality of communicable couple including absolute speed (Gleichauf I, col. 3, lines 18-20). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the absolute speed as the quality of communication couple to the system under test taught by Gleichauf '668 with Gleichauf '656 rule driven multi-phase network vulnerability assessment such as collecting data through port scans where speed processing is critical to prevent or minimize network bottlenecks.

Regarding to claims 104 and 105, these are method and computer program product claims respectively, of the claimed apparatus above (claim 103). Therefore, for reasons applied above, such claims also are obvious.

3. Claims 58, 62, 64, 68, 70 and 74 are rejected under 35 U.S.C. 103(a) as being unpatentable over Gleichauf (U.S. Patent No. 6,324,656) in view of Li et al. ("Effective load sharing on heterogeneous networks of workstations", Proceedings of 2000

International Parallel and Distributed processing Symposium, (IPDPS '00), May 2000, pp. 431-438).

Regarding claim 58, Gleichauf teaches an apparatus comprising:

a plurality of testers (Gleichauf, plurality of NVA engines; col. 3, lines 57-67);

wherein each of said plurality of testers is adapted to communicably couple to a system under test (Gleichauf, NVA engines each couple to the network being tested; col. 3, lines 43-50 and 57-63), a test system under test is performed by a selected tester of said plurality of testers (Gleichauf, iterative process determines whether second test is conducted as an active exploits test 98 by second NVA engine or as a further preliminary analysis test 94 by first NVA engine, wherein determination is based on information in port database 22/network map; Fig. 3A; col. 5, lines 36-40; col. 6, lines 8-12 and 34-37; col. 7, lines 55-61). Gleichauff do not teach the plurality of testers has a load balance characteristic describing a degree of balance of loads of testers wherein the selected tester is selected from plurality of testers based at least partially on optimizing the load balance characteristic. However, Li et al. teach using distributing parallel processing on heterogeneous networks of workstations as effective load sharing of workworks resource (Li, 3rd page 1). It would have been obvious to one of ordinary skill in the art at the time the invention was made to implement's Gleichauf's teaching of accessing network vulnerability with Li's teaching of implementing parallel processing to balance network workloads for sharing cpu and memory resources.

Regarding to claim 62, Gleichauf and Li teach all the limitations of claim 58, and further teach an apparatus:

Wherein each tester of said plurality of testers has at least one quality of communicable coupling to the system under test (Gleichauf, location of coupled NVA engine impacts access to devices on network; col. 3, lines 64-67); and

Wherein the selected tester is selected from said plurality of testers based at least partially on the selected tester's quality of communicable coupling (Gleichauf, it is inherent that certain NVA engines will be selected where they provide exclusive access to certain devices on a network; col. 3, lines 64-67).

Regarding claims 64, 68, 70 and 74, these are a computer-program product and method versions, respectively, of the claimed apparatus above (claims 58 and 62). Therefore, for reasons applied above, such claims also are anticipated.

Allowable Subject Matter

4. Claims 63, 69 and 75 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Regarding claims 63, 69 and 75, the closest prior art, Gleichauf '656 and '668, does not explain selecting a tester from a plurality of testers based on the quality of communicable coupling wherein the coupling includes cost per bit, absolute speed, and geographical proximity of the selected tester to the system under test.

While Gleichauf '656 teaches a plurality of testers (NVA engines running on servers) that are each coupled to different segments of the network, such that each tester represents a different geographical proximity to the system under test (col. 3, lines 57-

selection of a tester is based on its accessibility to devices rather than its geographical proximity, which do not necessarily equate to the same thing. The prior art makes no reference to the selection of a tester based on geographical proximity per se. The prior art also makes no reference to the selection of a tester based on the cost per bit or absolute speed of its communication coupling. Therefore, it would not seem obvious to one of ordinary skill in the art to provide for selecting a tester from a plurality of testers based on the quality of communicable coupling wherein the coupling includes cost per bit, absolute speed, and geographical proximity of the selected tester to the system under test because the prior art provides no motivation for selecting between testers on the basis of these qualities of communicable coupling, particularly where there plurality of testers from which to select is inhomogeneous.

Conclusion

5. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Tongoc Tran whose telephone number is (571) 272-3843. The examiner can normally be reached on 8:30-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory Morse can be reached on (571) 272-3838. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Examiner: Tongoc Tran
Art Unit: 2134

January 6, 2006

EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER